



Resolución Directoral

Resolución Directoral N° 1426-2018-JUS/DGTAIPD-DPDP

Expediente N°
016-2018-JUS/DPDP-PS

Resolución N° 1426-2018-JUS/DGTAIPD-DPDP

Lima, 26 de Junio de 2018

VISTOS:

El Informe N° 004-2017-JUS/DGPDP-DSC de fecha 11 de enero de 2016, que se sustenta en las Actas de Fiscalización N° 01-2016¹ y 02-2016² de 27 de octubre de 2016 y N° 03-2014³ de 28 de octubre de 2016 (Expediente de Fiscalización N° 16-2018-DSC), emitido por la Dirección de Supervisión y Control de la Dirección General de Protección de Datos Personales; el escrito de descargo presentado por la administrada; y demás documentos que obran en el respectivo expediente administrativo y;

CONSIDERANDO:

I. Antecedentes

1. Mediante Oficio N° 0051-2016/ILN-CPC-INDECOPI⁴ y anexos⁵ recibido el 24 de junio de 2016, la Comisión de Protección al Consumidor Sede Lima Norte del INDECOPI comunicó a la Dirección General de Protección de Datos Personales (DGPDP), una posible vulneración a la Ley N° 29733, Ley de Protección de Datos Personales (LPDP), en algunos casos de reclamación por falta de idoneidad en la entrega/devolución de tarjetas de crédito que efectuaba el BBVA.
2. Mediante Oficio N° 255-2016-JUS/DGPDP-DSC⁶ de 14 de setiembre de 2016, la Dirección de Supervisión y Control de la Dirección General de Protección de Datos Personales (en adelante, DSC), solicitó información adicional a BBVA Banco Continental con la finalidad de complementar la comunicación formulada por el INDECOPI.



M. GONZALEZ I

¹ Folio 80 a 84

² Folio 90 a 94

³ Folio 107 a 111

⁴ Folio 02

⁵ Folio 03 a 34

⁶ Folio 37

Resolución Directoral N° 1426-2018-JUS/DGTAIPD-DPDP

3. Mediante escrito presentado con hoja de tramite 57901-2016MSC⁷ y anexos⁸, BBVA Banco Continental absolvió el requerimiento emitido con Oficio N° 255-2016-JUS/DGPDP-DSC.
4. Mediante Resolución N° 1 de 25 de octubre de 2016⁹ se resolvió incluir en el procedimiento de fiscalización a Olva Courier S.A.C. (en adelante, la administrada) e Internacional Latinoamericana de Servicios S.A., así como ampliar el procedimiento de fiscalización al BBVA Banco Continental, Olva Courier S.A.C. e Internacional Latinoamericana de Servicios S.A.
5. Mediante Orden de Visita de Fiscalización N° 078-2016-JUS/DGPDP-DSC¹⁰ de fecha 26 de octubre de 2016, la DSC dispuso la realización de una visita de fiscalización a Olva Courier S.A.C.
6. Mediante el Acta de Fiscalización N° 01-2016¹¹, se deja constancia de los hechos verificados en la visita realizada a las instalaciones de la administrada, sito en: Calle Coppa N° 123, región Callao, distrito del Callao, provincia y departamento de Callao, el 27 de octubre de 2016 de horas 10:50 am a 01:15 pm.
7. Mediante Acta de Fiscalización N° 02-2016¹² y anexos¹³ se deja constancia de los hechos verificados en la visita realizada a las instalaciones de la administrada, sito en: Av. Argentina N° 4458, región Callao, distrito del Callao, provincia y departamento de Callao, el 27 de octubre de 2016 de horas 01:30 pm a 03:00 pm.
8. Mediante Orden de Visita de Fiscalización N° 079-2016-JUS/DGPDP-DSC¹⁴ de 26 de octubre de 2016, la DSC dispuso la realización de una visita de fiscalización a Internacional Latinoamericana de Servicios S.A.
9. Mediante Acta de Fiscalización N° 03-2014¹⁵ y anexos¹⁶ se deja constancia de los hechos verificados en la visita realizada a las instalaciones de Internacional Latinoamericana de Servicios S.A., sito en: Av. Argentina N° 3147, distrito de Cercado de Lima, provincia y departamento de Lima, el 28 de octubre de 2016 de horas 10:20 am a 11:40 am.
10. Mediante Informe N° 003-2017-DSC-ORQR¹⁷ de 06 de enero de 2016, se emitió el informe de la supervisión realizada a la administrada y a Internacional Latinoamericana de Servicios S.A.
11. Mediante Informe N° 004-2017-JUS/DGPDP-DSC¹⁸ recibido el 11 de enero de 2017, la DSC remitió a la Dirección de Sanciones de la Dirección General de Protección de Datos Personales (en adelante, DS), los resultados de la supervisión realizada a la administrada, adjuntando las actas mencionadas en el considerando precedente y demás documentos que conforman el expediente administrativo; dicho informe fue



⁷ Folio 38 a 39

⁸ Folio 40 a 71

⁹ Folio 72

¹⁰ Folio 74

¹¹ Folio 80 a 84

¹² Folio 90 a 94

¹³ Folio 95 a 100

¹⁴ Folio 101

¹⁵ Folio 107 a 111

¹⁶ Folio 112 a 115

¹⁷ Folio 119 a 120

¹⁸ Folio 121 a 123



Resolución Directoral

Resolución Directoral N° 1426-2018-JUS/DGTAIPD-DPDP

notificado a la administrada con Oficio N° 24-2017-JUS/DGPDP-DSC¹⁹ el 24 de enero de 2017.

12. Mediante Resolución Directoral N° 076-JUS/DGTAIPD-DFI²⁰ de fecha 29 de diciembre de 2017, notificada con Oficio N° 299-2017-JUS/DGTAIPD-DFI²¹ el 18 de enero de 2017, la Dirección de Fiscalización e Instrucción de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (en adelante, DFI), resolvió iniciar procedimiento administrativo sancionador a la administrada por la presunta comisión de la siguiente infracción:

- La administrada no habría cumplido con implementar las medidas de seguridad para el tratamiento de datos personales al:
 - No contar con procedimientos documentados de gestión de accesos, gestión de privilegios y verificación periódica de privilegios (incumpliendo lo establecido en el numeral 1 artículo 39 del RLPDP).
 - Verificarse que el equipo de cómputo asignado al ejecutivo de cuenta tiene acceso a internet sin restricciones sin restricciones pudiendo acceder a cualquier tipo de páginas incluyendo las de correo personal, lo que genera riesgos de duplicidad de los datos personales (incumpliendo lo establecido en el artículo 43 del RLPDP).



M. GONZÁLEZ L.

13. Mediante Oficio N° 299-2017-JUS/DGTAIPD-DFI²² recibido el 18 de enero de 2018, se notificó a la administrada la resolución que inicia el procedimiento administrativo sancionador.
14. Mediante escrito presentado con hoja de trámite 8751-2018MSC²³ y anexos²⁴ presentado el 07 de febrero de 2018, la administrada presentó su escrito de descargos.

¹⁹ Folio 124

²⁰ Folio 128 a 131

²¹ Folio 134

²² Folio 134

²³ Folio 135 a 146

²⁴ Folio 147 a 180

Resolución Directoral N° 1426-2018-JUS/DGTAIPD-DPDP

15. Mediante Proveído N° 02 de 23 de febrero de 2018, se dispuso adjuntar al expediente las copias de la documentación presentada por la administrada al expediente 26-2014-DSC relacionada a la gestión de accesos y gestión de privilegios, agregándose al presente expediente de folios 182 a 194.
16. Mediante Informe Técnico N° 45-2018-DFI-VARS²⁵ de fecha 23 de febrero de 2018, se emitió un informe complementario de evaluación de implementación de las medidas de seguridad de la administrada.
17. Mediante Oficio N° 128-2018-JUS/DGTAIPD-DFI²⁶ recibido el 28 de febrero de 2018, la DFI requirió a la administrada información adicional sobre el procedimiento de fiscalización; ello fue absuelto con la documentación adjunta al escrito presentado el 05 de marzo de 2018, con hoja de tramite 15312-2018MSC²⁷.
18. Mediante Informe Técnico N° 56-2018-DFI-VARS²⁸ de 12 de marzo de 2018, la DFI emitió informe de evaluación de implementación de las medidas de seguridad de la administrada.
19. Mediante Resolución Directoral N° 42-2018-JUS/DGTAIPD-DFI²⁹, de fecha 23 de marzo de 2018, notificada a la administrada con Oficio N° 219-2018-JUS/DGTAIPD-DFI³⁰, el 28 de marzo de 2018, la Dirección de Fiscalización e Instrucción, en virtud a lo establecido en el artículo 122 del Reglamento de la LPDP, cerró la etapa instructiva del procedimiento administrativo sancionador.
20. Con Informe N° 18-2018-JUS/DGTAIPD-DFI³¹ de 22 de marzo de 2018, notificado a la administrada con Oficio N° 219-2018-JUS/DGTAIPD³² el 28 de marzo de 2018, la DFI emitió el informe final de instrucción recomendando a la Dirección de Protección de Datos Personales, analizar lo siguiente:
 - (...) declarar la inexistencia de la presunta infracción, pues las actuaciones de instrucción han permitido verificar que la administrada contaba, antes de la imputación de cargos con las medidas de seguridad para el tratamiento de datos personales requeridas por los artículos 39° (numeral 1) y 43° del RLPDP, debiéndose archivar el procedimiento sin sanción.



M. GONZALEZ L

II. Competencia

21. Mediante Decreto Supremo N° 013-2017-JUS de fecha 21 de junio de 2017, se aprobó el Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos (ROF del MINJUS), derogando el Decreto Supremo N° 011-2012-JUS.
22. El artículo 70 del ROF del MINJUS crea la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales como órgano de línea encargado de ejercer la Autoridad Nacional de Protección de Datos Personales.

²⁵ Folio 195

²⁶ Folio 198

²⁷ Folio 199 a 209

²⁸ Folio 210 a 211

²⁹ Folio 212 a 213

³⁰ Folio 221

³¹ Folio 215 a 219

³² Folio 221



Resolución Directoral

Resolución Directoral N° 1426-2018-JUS/DGTAIPD-DPDP

23. Conforme a lo dispuesto en el artículo 74 del ROF del MINJUS, la Dirección de Protección de Datos Personales, es la unidad orgánica competente para resolver en primera instancia, los procedimientos administrativos sancionadores iniciados por la Dirección de Fiscalización e Instrucción.
24. Sin embargo, mediante Resolución Directoral N° 27-2018-JUS/DGTAIPD³³, se designó a la Sra. Anais Caridad Zavala Huaisara, Directora (e) de Transparencia y Acceso a la Información Pública, como autoridad administrativa que resolverá el procedimiento sancionador en primera instancia iniciado a OLVA COURRIER S.A.C., debido a que se aceptó la abstención presentada por la Directora de Protección de Datos Personales.
25. Dado que, la encargatura de la Dirección de Transparencia y Acceso a la Información Pública a la señora Anais Caridad Zavala Huaisara culminó el 03 de abril del presente; mediante Resolución Directoral N° 74-2018-JUS/DGTAIPD, se dejó sin efecto la abstención aceptada para resolver el procedimiento sancionador iniciado a OLVA COURRIER SA..C señalando que la autoridad administrativa que resolverá el mencionado procedimiento sancionador será la Directora de Protección de Datos Personales.
26. En tal sentido, en ejercicio de sus facultades, corresponde a la Dirección de Protección de Datos Personales de la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales determinar si se ha cometido infracción a la LPDP y a su Reglamento.



III. Normativa sancionadora aplicable

27. Mediante el Decreto Supremo N° 019-2017-JUS de fecha 15 de setiembre de 2017, se aprobó el reglamento del Decreto Legislativo N° 1353 que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el Régimen de Protección de Datos Personales y la regulación de la gestión de intereses (en adelante, Decreto Legislativo N° 1353).

³³ Folio 222 a 223

Resolución Directoral N° 1426-2018-JUS/DGTAIPD-DPDP

28. La Tercera Disposición Complementaria Modificatoria del mencionado reglamento incorpora el capítulo de infracciones al Título VI del Reglamento de la LPDP, agregando el artículo 132 que tipifica las infracciones.
29. Por su parte, el presente procedimiento sancionador se inició estando vigente el artículo 38 de la LPDP.
30. Entonces, el sistema jurídico ha permitido una excepción en torno al principio de irretroactividad³⁴ en materia penal y administrativo sancionador, conocido como la retroactividad benigna.
31. La retroactividad benigna se hace efectiva si luego de la comisión de un ilícito administrativo, se produce una modificación normativa y dicha norma establece una consecuencia más beneficiosa para el infractor, ya sea la destipificación o el establecimiento de una sanción menor, en comparación con la norma anterior (vigente al momento que se cometió la infracción), por lo que debe aplicarse retroactivamente la nueva norma. Cabe señalar, que la retroactividad debe ser el resultado de una evaluación integral por parte de la Administración y como tal debe verificarse los supuestos y requisitos que la norma exija de manera que produzca consecuencias jurídicas favorables para el administrado.
32. En este sentido, el artículo 2 del Decreto Legislativo N° 1272 modificó el principio de irretroactividad recogido en el TUO de la LPAG, en el cual se precisó los supuestos sobre los cuales se podría aplicar la excepción, siendo los siguientes:
- Tipificación de la infracción más favorable
 - Previsión de la sanción más favorable, incluso de aquellas que se encuentran en etapa de ejecución.
 - Plazos de prescripción más favorables.
33. En la línea de lo expuesto, apreciándose que los supuestos de hechos (incumplimiento de la obligación) en los cuales habría incurrido la administrada ha variado de tipificación y de sanción (al momento en que se detectó la infracción); en atención a la excepción (retroactividad benigna) establecida en el principio de irretroactividad que rige la potestad sancionadora administrativa, se aplicará la disposición que resulte más favorable al administrado.
34. Sobre la obligación de implementar las medidas de seguridad de la información de acuerdo a lo establecido en la LPDP y su Reglamento:

Norma	Regulación anterior	Regulación actual
Sustantiva	Obligación regulada en el artículo 39, y 43 del	Obligación regulada en el artículo 39, y 43 del

³⁴ Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N° 006-2017-JUS.

“Artículo 246.- Principios de la potestad sancionadora administrativa

La potestad sancionadora de todas las entidades está regida adicionalmente por los siguientes principios especiales: (...)

5.- Irretroactividad.- Son aplicables las disposiciones sancionadoras vigentes en el momento de incurrir el administrado en la conducta a sancionar, salvo que las posteriores le sean más favorables.

Las disposiciones sancionadoras producen efecto retroactivo en cuanto favorecen al presunto infractor o al infractor, tanto en lo referido a la tipificación de la infracción como a la sanción y a sus plazos de prescripción, incluso respecto de las sanciones en ejecución al entrar en vigor la nueva disposición. (El subrayado es nuestro)

(...)



Resolución Directoral

Resolución Directoral N° 1426-2018-JUS/DGTAIPD-DPDP

	Reglamento de la LPDP, aprobado mediante Decreto Supremo N° 003-2013-JUS, en concordancia con el artículo 9 de la LPDP.	Reglamento de la LPDP, aprobado mediante Decreto Supremo N° 003-2013-JUS, en concordancia con el artículo 9 de la LPDP.
Tipificadora	Literal a. del numeral 2 del artículo 38 de la LPDP, esto es: <i>"Dar tratamiento a los datos personales contraviniendo los principios establecidos en la presente Ley o incumpliendo sus demás disposiciones o las de su Reglamento"</i>	Literal a. del numeral 1 del artículo 132 del Reglamento de la LPDP, esto es: <i>"Realizar tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en la normativa sobre la materia"</i> .
Eventual sanción	Numeral 2 del artículo 39 de la LPDP que establece la infracción grave sancionada con más de 5 a 50 UIT.	Numeral 1 del artículo 39 de la LPDP que establece la infracción leve sancionada con 0,5 UIT hasta 5 UIT.



GONZALEZ I

35. En atención a lo anterior, cabe señalar que el incumplimiento de implementar las medidas de seguridad de la información, en la actual regulación de infracciones se subsume en una tipificación específica que comprende dicho hecho infractor, por lo que corresponde aplicar dicha tipificación.

Asimismo, se evidencia que el marco normativo actual (norma que entró en vigencia el 16 de setiembre de 2017) es más favorable para la administrada en comparación con la norma anterior a la fecha en la que se cometió la infracción (27 de octubre de 2016), toda vez que actualmente la sanción conforme a la tipificación resulta más beneficiosa al haber cambiado de grave a leve.

Resolución Directoral N° 1426-2018-JUS/DGTAIPD-DPDP

En ese sentido, en virtud de la excepción al principio de irretroactividad (retroactividad benigna) establecido en el artículo 246 del TUO de la LPAG³⁵, corresponde aplicar la tipificación más favorable a la administrada, esto es el literal a. del numeral 1 del artículo 132 del Reglamento de la LPDP: "Realizar tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en la normativa sobre la materia", al presunto incumplimiento de las disposiciones de los artículos 39 y 43 del Reglamento de la LPDP, al no haber implementado las medidas de seguridad de la información establecidas por tales normas.

36. De otro lado, acerca de la responsabilidad de la administrada, se debe tener en cuenta que el literal f) del numeral 1 del artículo 255³⁶ del Texto Único Ordenado de la Ley del Procedimiento Administrativo General, aprobado mediante Decreto Supremo N° 006-2017-JUS (en adelante, LPAG), establece como una causal eximente de la responsabilidad por infracciones, la subsanación voluntaria del acto imputado como infractor, si es realizada de forma previa a la notificación de imputación de cargos.
37. Asimismo, se debe atender a lo dispuesto en el artículo 126³⁷ del Reglamento de la LPDP, que considera como atenuantes la colaboración con las acciones de la autoridad y el reconocimiento espontáneo de las infracciones conjuntamente con la adopción de medidas de enmienda; dichas atenuantes, de acuerdo con la oportunidad del reconocimiento y las fórmulas de enmienda puede permitir la reducción motivada de la sanción por debajo del rango previsto en la LPDP.
38. Dicho artículo debe leerse conjuntamente con lo previsto en el numeral 2 del artículo 255³⁸ de la LPAG, que establece como condición atenuante el reconocimiento de la responsabilidad por parte del infractor de forma expresa y por escrito, debiendo



M. GONZÁLEZ L.

³⁵ Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N° 006-2017-JUS.

"Artículo 246.- Principios de la potestad sancionadora administrativa

La potestad sancionadora de todas las entidades está regida adicionalmente por los siguientes principios especiales: (...)

5.- Irretroactividad.-Son aplicables las disposiciones sancionadoras vigentes en el momento de incurrir el administrado en la conducta a sancionar, salvo que las posteriores le sean más favorables.

Las disposiciones sancionadoras producen efecto retroactivo en cuanto favorecen al presunto infractor o al infractor, tanto en lo referido a la tipificación de la infracción como a la sanción y a sus plazos de prescripción, incluso respecto de las sanciones en ejecución al entrar en vigor la nueva disposición.

(...)"

³⁶ Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N° 006-2017-JUS.

"Artículo 255.- Eximentes y atenuantes de responsabilidad por infracciones

1.- Constituyen condiciones eximentes de la responsabilidad por infracciones las siguientes:

(...)

f) La subsanación voluntaria por parte del posible sancionado del acto u omisión imputado como constitutivo de infracción administrativa, con anterioridad a la notificación de la imputación de cargos a que se refiere el inciso 3) del artículo 253."

³⁷ Reglamento de la Ley de Protección de Datos Personales, aprobado por Decreto Supremo N° 003-2013-JUS.

"Artículo 126.- Atenuantes.

La colaboración con las acciones de la autoridad y el reconocimiento espontáneo de las infracciones acompañado de acciones de enmienda se considerarán atenuantes. Atendiendo a la oportunidad del reconocimiento y a las fórmulas de enmienda, la atenuación permitirá incluso la reducción motivada de la sanción por debajo del rango previsto en la Ley"

³⁸ Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N° 006-2017-JUS.

"Artículo 255.- Eximentes y atenuantes de responsabilidad por infracciones

(...)

2.- Constituyen condiciones atenuantes de la responsabilidad por infracciones las siguientes:

a) Si iniciado un procedimiento administrativo sancionador el infractor reconoce su responsabilidad de forma expresa y por escrito.

En los casos en que la sanción aplicable sea una multa esta se reduce hasta un monto no menor de la mitad de su importe.

b) Otros que se establezcan por norma especial."



Resolución Directoral

Resolución Directoral N° 1426-2018-JUS/DGTAIPD-DPDP

reducir la multa a imponérsele hasta no menos de la mitad del monto de su importe; y por otro lado, las que se contemplen como atenuantes en las normas especiales.

IV. Análisis de la cuestión en discusión

39. Para emitir pronunciamiento en el presente caso, se debe determinar si la administrada no habría implementado las medidas de seguridad consistentes en:

- (a) Contar con procedimientos documentados de gestión de accesos, gestión de privilegios y verificación periódica, de acuerdo al numeral 1 del artículo 39 del RLPDP.
- (b) Verificar que el equipo de cómputo asignado al ejecutivo de cuenta tenía acceso a internet sin restricciones a fin de evitar riesgos de duplicidad de los datos personales, de acuerdo al artículo 43 del RLPDP.



Y si en consecuencia, la administrada incurrió en la infracción leve tipificada en el literal a. del numeral 1 del artículo 132 del Reglamento de la LPDP: *“Realizar tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en la normativa sobre la materia”*.

Sobre el deber de cumplir con las medidas de seguridad

40. Se imputa a la administrada que no habría implementado las medidas de seguridad de la información establecidas en los artículos 39 y 43 del RLPDP, por haber incurrido presuntamente en los hechos descritos en el numeral 38 de la presente resolución; configurándose la infracción leve tipificada en el literal a. del numeral 1 del artículo 132 del Reglamento de la LPDP consistente en: *“Realizar tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en la normativa sobre la materia”*.

En tal sentido corresponde analizar la normativa vigente y aplicable sobre la materia, los medios probatorios que dejan constancia de los hallazgos encontrados en el

Resolución Directoral N° 1426-2018-JUS/DGTAIPD-DPDP

procedimiento, y los descargos presentados por la administrada para desvirtuar el hecho imputado.

41. Previo a ello, es preciso recordar que el artículo 9 de la LPDP señala el principio de seguridad como uno de los principios rectores de la protección de datos personales:

“Artículo 9. Principio de seguridad

El titular del banco de datos personales y el encargado de su tratamiento deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate.”

42. Asimismo, el artículo 16 de la LPDP establece la obligación de adoptar medidas de seguridad para el tratamiento de datos personales:

“Artículo 16. Seguridad del tratamiento de datos personales

Para fines del tratamiento de datos personales, el titular del banco de datos personales debe adoptar medidas técnicas, organizativas y legales que garanticen su seguridad y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

(...)

Queda prohibido el tratamiento de datos personales en bancos de datos que no reúnan los requisitos y las condiciones de seguridad a que se refiere este artículo.”

Sobre el incumplimiento del numeral 1 del artículo 39 y el artículo 43 del RLPDP

43. Se imputa a la administrada la comisión de los siguientes hechos:

- (i) no habría documentado los procedimientos de gestión de accesos, gestión de privilegios y verificación periódica de privilegios asignados a los usuarios del sistema, de acuerdo al numeral 1 del artículo 39 del RLPDP.
- (ii) no habría verificado que el equipo de cómputo asignado al ejecutivo de cuenta tenía acceso a internet sin restricciones con lo que se estaría generando riesgo de duplicidad de los datos personales, de acuerdo al artículo 43 del RLPDP.

44. Así pues, respecto de las medidas de seguridad a adoptarse en el tratamiento de datos personales en soporte automatizado, el Reglamento de la LPDP señala lo siguiente:

“Artículo 39.- Seguridad para el tratamiento de la información digital.

Los sistemas informáticos que manejen bancos de datos personales deberán incluir en su funcionamiento:

1. *El control de acceso a la información de datos personales incluyendo la gestión de accesos desde el registro de un usuario, la gestión de los privilegios de dicho usuario, la identificación del usuario ante el sistema, entre los que se encuentran usuario, contraseña, uso de certificados digitales, tokens, entre otros, y realizar una verificación periódica de los privilegios asignados, los cuales deben estar definidos mediante un procedimiento documentado a fin de garantizar su idoneidad.”*





Resolución Directoral

Resolución Directoral N° 1426-2018-JUS/DGTAIPD-DPDP

De ello se desprende que es obligatorio definir procedimientos documentados de gestión de accesos y gestión de privilegios de los usuarios para el acceso al sistema, la identificación de usuarios en el sistema, así como el proceso de verificación periódica de dichos privilegios, esto es, se debe establecer el procedimiento para el alta, baja y modificación de datos, modificación de usuarios, así como sus privilegios en el sistema.

45. De otro lado, respecto de las medidas de seguridad a adoptarse en el tratamiento de datos personales, el Reglamento de la LPDP señala lo siguiente:

“Artículo 43.- Copia o reproducción.

La generación de copias o la reproducción de los documentos únicamente podrán ser realizadas bajo el control del personal autorizado.

Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior. (...).”

De lo anterior se desprende que las copias generadas o la reproducción de documentos solo se podrán realizar bajo el control de personal autorizado.

46. Ahora bien, del Acta de Fiscalización N° 01-2016³⁹ en la cual se deja constancia de la supervisión realizada a la administrada el día 27 de octubre de 2016, se indica lo siguiente:

“(…) Se verificaron las medidas de seguridad en el equipo de cómputo asignado al ejecutivo de cuenta (encargado de la seguridad de la información de los clientes de tarjeta de crédito del BBVA Banco Continental), constatándose lo siguiente: (...) 4) cuenta con acceso a internet sin ninguna restricción (puede acceder a todo tipo de página web) (...).

La entidad visitada indicó que no cuenta con procedimientos documentados referentes a la gestión de accesos y gestión de privilegios; asimismo, indicó que no cuenta con documentación referente a la verificación de privilegios asignados (...).”

³⁹ Folio 80 a 84



Resolución Directoral N° 1426-2018-JUS/DGTAIPD-DPDP

47. Por otro lado, con Informe N° 003-2017-DSC-ORQR⁴⁰ de fecha 06 de enero de 2016, se informó sobre la visita de fiscalización a la administrada indicando lo siguiente:

“V. Conclusiones

(...)

- 1. Olva Courier S.A.C. no documenta los procedimientos de gestión de accesos, gestión de privilegios y verificación periódica de privilegios incumpliendo con el numeral 1 del artículo 39 del Reglamento de la LPDP.*
- 2. Olva Courier S.A.C. no establece procedimientos que restrinjan la generación de copias o reproducción de documentos, incumpliendo el artículo 43 del Reglamento de la LPDP (...).”*

48. Con el Informe N° 004-2017-JUS/DGPDP-DSC⁴¹ de fecha 11 de enero de 2017, se informa sobre el procedimiento de fiscalización a la administrada, indicando lo siguiente:

“V. Conclusiones

- 1. Olva Courier S.A.C. no cuenta con las medidas de seguridad necesarias para la protección de los datos personales de los clientes (...), hecho que constituye una infracción de conformidad con el literal a) del numeral 2 del artículo 38 de la LPDP (...).”*

49. Posteriormente, el 07 de febrero de 2018 la administrada presentó sus descargos⁴² con hoja de trámite 8751-2018MSC señalando que en una fiscalización anterior realizada a sus instalaciones, a través del Acta N° 07-2014 y el Informe N° 063-2015-JUS/DGPDP-DSC de 15 de abril de 2015 recaídos en el Expediente N° 026-2014-DSC se determinó que cumplía las medidas de seguridad indicando que sus máquinas estaban bloqueadas y sin acceso a internet y que no habían indicios de infracción para iniciar procedimiento sancionador; señala que siempre contó con la documentación que acreditaba tales medidas (lo que sustenta con el cargo de la carta de 03 de marzo de 2015) pero que no la tenía a su alcance al momento de la fiscalización.

50. A fin de verificar los argumentos expuestos, con Proveído N° 02⁴³ de 23 de febrero de 2018, la DFI dispuso que se adjunten copias de la documentación del Expediente N° 026-2014-DSC al presente expediente, lo que consta de folios 182 a 194, lo que se evaluó en el Informe Técnico N° 45-2018-DFI-VARS⁴⁴ de 23 de febrero de 2018 indicando que *“(...) Olva Courier S.A.C. deberá remitir los procedimientos de gestión de accesos, gestión de privilegios y revisión periódica de privilegios asignados requerida en el numeral 1 del artículo 39 del Reglamento de la LPDP. Dichos documentos deberán corresponder a la fecha de inicio del procedimiento de fiscalización del expediente 034-2016-DSC.”*, documentación que fue requerida con Oficio N° 128-2018-JUS/DGTAIPD-DFI⁴⁵.

51. En atención a lo anterior, con escrito remitido con hoja de trámite 15312-2018MSC⁴⁶ la administrada remitió la documentación solicitada indicando que aquella se encontraba y se encuentra actualmente siendo aplicada por su organización; por lo

⁴⁰ Folio 119 a 120

⁴¹ Folio 121 a 123

⁴² Folio 135 a 180

⁴³ Folio 181

⁴⁴ Folio 195

⁴⁵ Folio 198

⁴⁶ Folio 199 a 209



Resolución Directoral

Resolución Directoral N° 1426-2018-JUS/DGTAIPD-DPDP

que a fin de evaluar la documentación referida, se emitió el Informe Técnico N° 56-2018-DFI-VARS⁴⁷ en el cual se señala lo siguiente:

“III. (...).

1. Respecto a la obligación de tener documentado la gestión de accesos, gestión de privilegios y verificación periódica de privilegios, Olva Courier S.A.C. a través de la documentación remitida el día 03 de marzo de 2015 cumple con documentar la gestión de accesos, gestión de privilegios y la revisión periódica de privilegios asignados debido a que define políticas de seguridad de accesos a los servicios a los servicios y aplicaciones a través perfiles. Por lo que estaría cumpliendo con el numeral 1 del artículo 39 del Reglamento de la LPDP.

2. Con sus descargos de 05 de marzo de 2018 Olva Courier S.A.C. presenta los documentos “copia de las normativas de uso del computador y sistema de aplicación”, “copia de la política de seguridad de información”, “copia de los lineamientos de seguridad de la información”, “copia de la política de acceso a aplicaciones” y “copia de la política de accesos a base de datos” a través de la cual señala la seguridad para acceder al sistema que realiza tratamiento de datos personales el que es realizado por medio de perfiles determinados. Asimismo, define perfiles y funciones a los usuarios en el sistema, además señala que el usuario con perfil administrador es el encargado de los perfiles de cada aplicación. Por lo que estaría cumpliendo con el numeral 1 del artículo 39 del Reglamento de la LPDP.

3. Finalmente, lo referido a establecer procedimientos de medidas de seguridad que restrinja la generación de copias o reproducción de documentos, Olva Courier S.A.C. durante el inicio del procedimiento de fiscalización ya contaba con políticas de seguridad las cuales son remitidas a través de sus descargos donde establece las políticas de seguridad para el no uso de USB/CD/DVD o algún dispositivo de intercambio de información, así como políticas de confidencialidad para el personal involucrado en el tratamiento de datos personales. Cabe señalar que la transmisión de información por internet es realizada bajo encriptación. En ese sentido, estaría cumpliendo en lo que dispuesto en el artículo 43 del Reglamento de la LPDP.”



M. GONZALEZ L.

⁴⁷ Folio 210 a 211

Resolución Directoral N° 1426-2018-JUS/DGTAIPD-DPDP

52. De acuerdo a los documentos descritos anteriormente, se observa que al año 2015, la administrada cumplía con la medidas de seguridad referidas a la documentación de procedimientos de gestión de accesos, gestión de privilegios y verificación periódica de privilegios, lo que se acredita con la documentación presentada al Expediente N° 026-2014-DSC a través de la Carta de fecha 03 de marzo de 2015⁴⁸ que se adjunta al presente procedimiento y respecto de la cual el Informe Técnico N° 56-2018-DFI-VARS⁴⁹ de 12 de marzo de 2018 concluye que cumple con lo establecido en el numeral 1 del artículo 29 del Reglamento de la LPDP.
53. Asimismo, se aprecia que con el escrito presentado con hoja de trámite 15312-2018MSC el 05 de marzo de 2018⁵⁰, la administrada adjunta copia de las normativas de uso del computador y sistema de aplicación⁵¹, copia de la política de seguridad de información⁵², copia de los lineamientos de seguridad de la información⁵³, copia de la política de acceso a aplicaciones⁵⁴ y copia de la política de accesos a base de datos⁵⁵, todos de fecha 01 de setiembre de 2016, con los que se acredita el cumplimiento de la medidas de seguridad del numeral 1 del artículo 39 en el presente procedimiento, lo que también se aprecia del Informe Técnico N° 56-2018-DFI-VARS⁵⁶.
54. De otro lado, en cuanto a las políticas y controles de restricción de copias de datos personales, y controles de acceso a internet a fin de evitar riesgos de duplicidad de información, de acuerdo al Informe Técnico N° 56-2018-DFI-VARS⁵⁷ se concluye que la transmisión de información por internet es realizada bajo encriptación, con lo que cumple con lo establecido en el artículo 43 del Reglamento de la LPDP.
55. De lo expuesto se concluye que al momento de la fiscalización el 27 de octubre de 2016, la administrada si cumplía con las medidas de seguridad establecidas en los artículos 39 numeral 1 y 43 del Reglamento de la LPDP, ya que los documentos que acreditan tales medidas datan desde el año 2015 y son confirmados a través de la documentación del 01 de setiembre de 2016 que se adjunta, por lo que corresponde declarar la inexistencia de responsabilidad por parte de la administrada respecto de la imputación efectuada.

Por las consideraciones expuestas y de conformidad con lo dispuesto por la Ley N° 29733, Ley de Protección de Datos Personales, su reglamento aprobado por el Decreto Supremo N° 003-2013-JUS, el Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N° 006-2017-JUS, y el Reglamento del Decreto Legislativo N° 1353 que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el Régimen de Protección de Datos Personales y la regulación de la gestión de intereses, aprobado por Decreto Supremo N° 019-2017-JUS;

⁴⁸ Folio 183 a 194

⁴⁹ Folio 210 a 211

⁵⁰ Folio 199 a 201

⁵¹ Folio 202

⁵² Folio 203

⁵³ Folio 204 a 205

⁵⁴ Folio 206 a 207

⁵⁵ Folio 208 a 209

⁵⁶ Folio 210 a 211

⁵⁷ Folio 210 a 211



Resolución Directoral

Resolución Directoral N° 1426-2018-JUS/DGTAIPD-DPDP

SE RESUELVE:

Artículo 1.- Declarar la **Inexistencia** de la infracción tipificada en el literal a. del numeral 1 del artículo 132 del Reglamento de la LPDP “Realizar tratamiento de datos personales incumpliendo las medidas de seguridad establecidas en la normativa sobre la materia”; ya que no se acreditó el incumplimiento de las medidas de seguridad establecidas en el numeral 1 del artículo 39 y el artículo 43 del Reglamento de la LPDP.

Artículo 2.- Notificar a **OLVA COURIER S.A.C.** que contra la presente resolución, de acuerdo a lo indicado en el artículo 216 del Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N° 006-2017-JUS, proceden los recursos de reconsideración o apelación dentro de los quince (15) días hábiles posteriores a su notificación⁵⁸.

Artículo 3.- Notificar a **OLVA COURIER S.A.C.** la presente resolución, en su domicilio sito en: Av. Argentina N° 4458, Callao.

Regístrese y comuníquese.

MARIA ALEJANDRA GONZALEZ LUNA
Directora (e) de la Dirección de Protección de
Datos Personales
Ministerio de Justicia y Derechos Humanos

⁵⁸ Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N° 006-2017-JUS

Artículo 216. Recursos administrativos

216.1 Los recursos administrativos son:

a) Recurso de reconsideración
b) Recurso de apelación

Solo en caso que por ley o decreto legislativo se establezca expresamente, cabe la interposición del recurso administrativo de revisión.

216.2 El término para la interposición de los recursos es de quince (15) días perentorios, y deberán resolverse en el plazo de treinta (30) días.”